

Ring class fields by smaller generators

JA KYUNG KOO, DONG HWA SHIN AND DONG SUNG YOON

Abstract

We generate ring class fields of imaginary quadratic fields in terms of the special values of certain eta-quotients, which are related to the relative norms of Siegel-Ramachandra invariants (Theorem 4.4). These give us minimal polynomials with relatively small coefficients from which we are able to solve certain quadratic Diophantine equations concerning non-convenient numbers (Remark 5.4).

1 Introduction

Let K be an imaginary quadratic field of discriminant d_K . We set

$$(1) \quad \tau_K = \begin{cases} (-1 + \sqrt{d_K})/2 & \text{if } d_K \equiv 1 \pmod{4}, \\ \sqrt{d_K}/2 & \text{if } d_K \equiv 0 \pmod{4}, \end{cases}$$

which belongs to the complex upper half-plane \mathbb{H} and generates the ring of integers \mathcal{O}_K of K over \mathbb{Z} . Let $\mathcal{O} = [N\tau_K, 1]$ be the order of conductor N (≥ 1) in K . As a consequence of the main theorem of complex multiplication, the singular value $j(\mathcal{O}) = j(N\tau_K)$ of the elliptic modular function $j(\tau)$ generates the ring class field $H_{\mathcal{O}}$ of the order \mathcal{O} over K ([9, Chapter 10, Theorem 5] or [16, Theorem 5.7]). However, its minimal polynomial has too large integer coefficients to handle in practical use (see [1, Theorem 9.2 and §13.A]).

The *Dedekind eta-function* and *modular discriminant function* are defined by

$$(2) \quad \eta(\tau) = q^{1/24} \prod_{n=1}^{\infty} (1 - q^n) \quad \text{and} \quad \Delta(\tau) = (2\pi)^{12} \eta(\tau)^{24} \quad (\tau \in \mathbb{H}, q = e^{2\pi i \tau}),$$

2010 *Mathematics Subject Classification*. Primary 11G16; Secondary 11F03, 11G15, 11R37.

Key words and phrases. Class field theory, complex multiplication, elliptic and modular units.

The first named author was partially supported by the NRF of Korea grant funded by MISP (2013042157). The second named author was supported by Hankuk University of Foreign Studies Research Fund of 2014.

respectively. Under certain conditions, Enge and Schertz ([2] and [12]) constructed primitive generators of $H_{\mathcal{O}}$ over K in terms of the special values of η - and Δ -quotients (see also [14, §6.6–6.7]).

Let $N (\geq 2)$ be an integer with prime factorization $N = \prod_{k=1}^m p_k^{r_k}$. For each subset S of $\{1, \dots, m\}$ we set

$$(3) \quad P_S = \begin{cases} 1 & \text{if } S = \emptyset, \\ \prod_{k \in S} p_k & \text{if } S \neq \emptyset, \end{cases}$$

and let

$$(4) \quad P_N = \prod_{k=1}^m (p_k - 1), \quad \nu_N = \begin{cases} p_1 & \text{if } m = 1, \\ 1 & \text{if } m \geq 2, \end{cases} \quad \mu_N = \begin{cases} 2 & \text{if } m = 1 \text{ and } p_1 \equiv 1 \pmod{8}, \\ 1 & \text{otherwise.} \end{cases}$$

And, for each nontrivial ideal \mathfrak{f} of \mathcal{O}_K we consider the canonical homomorphism

$$\pi_{\mathfrak{f}} : \mathcal{O}_K \rightarrow \mathcal{O}_K / \mathfrak{f}.$$

In this paper we shall prove that if the order of the group

$$\pi_{p_k^{r_k} \mathcal{O}_K}(\mathcal{O}_K)^{\times} / \pi_{p_k^{r_k} \mathcal{O}_K}(\mathcal{O}_K^{\times}) \pi_{p_k^{r_k} \mathcal{O}_K}(\mathbb{Z})^{\times}$$

is greater than 2 for each $k \in \{1, \dots, m\}$, then the special value

$$\nu_N^{12\mu_N / \gcd(24, P_N)} \prod_{S \subseteq \{1, \dots, m\}} \eta((N/P_S)\tau_K)^{24(-1)^{|S|}\mu_N / \gcd(24, P_N)}$$

generates $H_{\mathcal{O}}$ over K (Theorem 4.4 and Remark 4.5). This ring class invariant is a real algebraic integer whose minimal polynomial has relatively small coefficients (Examples 5.1, 5.2, 5.3). To this end we shall further improve Schertz's idea [13] on characters of class groups (Lemmas 3.3 and 3.4) when utilizing the second Kronecker limit formula concerning Siegel-Ramachandra invariants (Proposition 4.1).

2 Eta-quotients

We shall show that the special values of certain η -quotients lie in the ring class fields of imaginary quadratic fields.

LEMMA 2.1. *Let $N (\geq 2)$ be an integer. Assume that a family of integers $\{m_d\}_{d|N}$, where d runs over all positive divisors of N , satisfies the following conditions:*

$$(i) \quad \sum_{d|N} m_d = 0.$$

$$(ii) \sum_{d|N} dm_d \equiv \sum_{d|N} (N/d)m_d \equiv 0 \pmod{24}.$$

$$(iii) \prod_{d|N} d^{m_d} \text{ is a square in } \mathbb{Q}.$$

Then the η -quotient

$$f(\tau) = \prod_{d|N} \eta(d\tau)^{m_d}$$

is a meromorphic modular function on $\Gamma_0(N) = \{\gamma \in \mathrm{SL}_2(\mathbb{Z}) \mid \gamma \equiv \begin{bmatrix} * & * \\ 0 & * \end{bmatrix} \pmod{N}\}$.

PROOF. See [10, Theorem 1.64]. □

REMARK 2.2. By the definition (2) we see the following identity

$$f(\tau) = q^{(1/24) \sum_{d|N} dm_d} \prod_{d|N} \prod_{n=1}^{\infty} (1 - q^{dn})^{m_d}.$$

So, $f(\tau)$ has rational Fourier coefficients with respect to q and has neither zeros nor poles on \mathbb{H} .

PROPOSITION 2.3. Let $N (\geq 2)$ be an integer with prime factorization $N = \prod_{k=1}^m p_k^{r_k}$. With the same notations as in (3) and (4), the η -quotient

$$g(\tau) = \prod_{S \subseteq \{1, \dots, m\}} \eta((N/P_S)\tau)^{24(-1)^{|S|} \mu_N / \gcd(24, P_N)}$$

is a weakly holomorphic modular function on $\Gamma_0(N)$ with rational Fourier coefficients.

PROOF. By Lemma 2.1 it suffices to show that

- (i) $\sum_{S \subseteq \{1, \dots, m\}} (-1)^{|S|} = 0$,
- (ii) $\sum_{S \subseteq \{1, \dots, m\}} (N/P_S)(-1)^{|S|} \equiv \sum_{S \subseteq \{1, \dots, m\}} (P_S)(-1)^{|S|} \equiv 0 \pmod{P_N}$,
- (iii) $\prod_{S \subseteq \{1, \dots, m\}} (N/P_S)^{24(-1)^{|S|} \mu_N / \gcd(24, P_N)}$ is a square in \mathbb{Q} .

First, we obtain that

$$\sum_{S \subseteq \{1, \dots, m\}} (-1)^{|S|} = \sum_{\ell=0}^m \sum_{|S|=\ell} (-1)^{|S|} = \sum_{\ell=0}^m \binom{m}{\ell} (-1)^\ell = 0.$$

Next, we derive that

$$\begin{aligned}
\sum_{S \subseteq \{1, \dots, m\}} (N/P_S)(-1)^{|S|} &= \sum_{\ell=0}^m \sum_{|S|=\ell} (N/P_S)(-1)^{|S|} \\
&= N \sum_{\ell=0}^m (-1)^\ell \sum_{|S|=\ell} 1/P_S \\
&= N \prod_{k=1}^m (1 - 1/p_k) \\
&= (N/p_1 p_2 \cdots p_m) \prod_{k=1}^m (p_k - 1) \\
&\equiv 0 \pmod{P_N},
\end{aligned}$$

and in a similar way we get

$$\sum_{S \subseteq \{1, \dots, m\}} P_S(-1)^{|S|} = \sum_{\ell=0}^m \sum_{|S|=\ell} P_S(-1)^{|S|} = \sum_{\ell=0}^m (-1)^\ell \sum_{|S|=\ell} P_S = \prod_{k=1}^m (1 - p_k) \equiv 0 \pmod{P_N}.$$

Lastly, we deduce that

$$\begin{aligned}
\prod_{S \subseteq \{1, \dots, m\}} (N/P_S)^{24(-1)^{|S|}\mu_N / \gcd(24, P_N)} &= \prod_{S \subseteq \{1, \dots, m\}} P_S^{-24(-1)^{|S|}\mu_N / \gcd(24, P_N)} \quad \text{by (i)} \\
&= (p_1 \cdots p_m)^{(\sum_{\ell=0}^{m-1} \binom{m-1}{\ell} (-1)^\ell) 24\mu_N / \gcd(24, P_N)} \\
&= \begin{cases} p_1^{24\mu_N / \gcd(24, p_1 - 1)} & \text{if } m = 1, \\ 1 & \text{if } m \geq 2, \end{cases}
\end{aligned}$$

which is a square in \mathbb{Q} by the definition of μ_N in (4). This proves the proposition. \square

For a positive integer N let \mathcal{F}_N be the field of meromorphic modular functions on $\Gamma(N) = \{\gamma \in \text{SL}_2(\mathbb{Z}) \mid \gamma \equiv I_2 \pmod{N}\}$ whose Fourier coefficients with respect to $q^{1/N}$ lie in $\mathbb{Q}(\zeta_N)$, where $\zeta_N = e^{2\pi i/N}$. Then it is well-known that \mathcal{F}_N is a Galois extension of $\mathcal{F}_1 = \mathbb{Q}(j(\tau))$ whose Galois group is isomorphic to

$$\text{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\} = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & d \end{bmatrix} \mid d \in (\mathbb{Z}/N\mathbb{Z})^\times \right\} \cdot \text{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\}.$$

Let $h(\tau) = \sum_{n > -\infty} c_n q^{n/N} \in \mathcal{F}_N$ with $c_n \in \mathbb{Q}(\zeta_N)$. The matrix $\begin{bmatrix} 1 & 0 \\ 0 & d \end{bmatrix}$ with $d \in (\mathbb{Z}/N\mathbb{Z})^\times$ acts on $h(\tau)$ by

$$h(\tau)^{\begin{bmatrix} 1 & 0 \\ 0 & d \end{bmatrix}} = \sum_{n > -\infty} c_n^{\sigma_d} q^{n/N},$$

where σ_d is the automorphism of $\mathbb{Q}(\zeta_N)$ given by $\zeta_N^{\sigma_d} = \zeta_N^d$. Now, let $\alpha \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\}$. Take a preimage $\tilde{\alpha} \in \mathrm{SL}_2(\mathbb{Z})$ of α with respect to the reduction $\mathrm{SL}_2(\mathbb{Z}) \rightarrow \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\}$. Then, α acts on $h(\tau)$ by the fractional linear transformation of $\tilde{\alpha}$ [9, Chapter 6, Theorem 3].

Throughout this paper we let K be an imaginary quadratic field of discriminant d_K with ring of integers \mathcal{O}_K and τ_K be as in (1). For a nontrivial ideal \mathfrak{f} of \mathcal{O}_K we denote by

$$\begin{aligned} I_K(\mathfrak{f}) &= \text{the group of fractional ideals of } K \text{ prime to } \mathfrak{f}, \\ P_{K,1}(\mathfrak{f}) &= \langle x\mathcal{O}_K \mid x \in \mathcal{O}_K \text{ such that } x \equiv 1 \pmod{\mathfrak{f}} \rangle. \end{aligned}$$

In particular, if $\mathfrak{f} = N\mathcal{O}_K$ for a positive integer N , then we further denote by

$$P_{K,\mathbb{Z}}(\mathfrak{f}) = \langle x\mathcal{O}_K \mid x \in \mathcal{O}_K \text{ such that } x \equiv n \pmod{\mathfrak{f}} \text{ for some } n \in \mathbb{Z} \text{ prime to } N \rangle.$$

By the existence theorem of class field theory there exists a unique abelian extension $K_{\mathfrak{f}}$ of K , called the *ray class field* of K modulo \mathfrak{f} , whose Galois group $\mathrm{Gal}(K_{\mathfrak{f}}/K)$ is isomorphic to the ray class group $\mathrm{Cl}(\mathfrak{f}) = I_K(\mathfrak{f})/P_{K,1}(\mathfrak{f})$ modulo \mathfrak{f} via the Artin reciprocity map $\sigma_{\mathfrak{f}} : \mathrm{Cl}(\mathfrak{f}) \rightarrow \mathrm{Gal}(K_{\mathfrak{f}}/K)$ [4, Chapters IV and V]. In particular, if $\mathfrak{f} = \mathcal{O}_K$, then $K_{\mathfrak{f}}$ becomes the Hilbert class field H_K of K , that is, the maximal unramified abelian extension of K .

Now, we let $\mathfrak{f} = N\mathcal{O}_K$ for a positive integer N . As a consequence of the main theorem of complex multiplication we obtain

$$(5) \quad H_K = K(j(\tau_K)) \quad \text{and} \quad K_{\mathfrak{f}} = K(h(\tau_K) \mid h(\tau) \in \mathcal{F}_N \text{ is finite at } \tau_K)$$

[9, Chapter 10, Theorem 1 and Corollary to Theorem 2]. Let $\min(\tau_K, \mathbb{Q}) = X^2 + bX + c$ and define a subgroup $W_{K,N}$ of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ by

$$W_{K,N} = \left\{ \begin{bmatrix} t - bs & -cs \\ s & t \end{bmatrix} \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \mid t, s \in \mathbb{Z}/N\mathbb{Z} \right\}.$$

By Shimura's reciprocity law we have the surjection

$$\begin{aligned} W_{K,N} &\rightarrow \mathrm{Gal}(K_{\mathfrak{f}}/H_K) \\ \gamma &\mapsto (h(\tau_K) \mapsto h^{\gamma}(\tau_K) \mid h(\tau) \in \mathcal{F}_N \text{ is finite at } \tau_K) \end{aligned}$$

whose kernel is

$$T_{K,N} = \begin{cases} \langle \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \rangle & \text{if } K = \mathbb{Q}(\sqrt{-1}), \\ \langle \begin{bmatrix} 1 & 1 \\ -1 & 0 \end{bmatrix} \rangle & \text{if } K = \mathbb{Q}(\sqrt{-3}), \\ \langle -I_2 \rangle & \text{if } K \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3}) \end{cases}$$

([16, Theorem 6.31 and Proposition 6.34] and [17, §3]).

On the other hand, let $\mathcal{O} = [N\tau_K, 1]$ be the order of conductor N in K . Then the ideal class group $C(\mathcal{O}) = I(\mathcal{O})/P(\mathcal{O})$ of the order \mathcal{O} , where $I(\mathcal{O})$ is the group of proper fractional \mathcal{O} -ideals and $P(\mathcal{O})$ is the subgroup of principal \mathcal{O} -ideals, is isomorphic to $I_K(\mathfrak{f})/P_{K,\mathbb{Z}}(\mathfrak{f})$ [1, §7.A and Proposition 7.22]. The *ring class field* $H_{\mathcal{O}}$ of the order \mathcal{O} is defined to be the unique abelian extension of K whose Galois group satisfies

$$(6) \quad \text{Gal}(H_{\mathcal{O}}/K) \simeq C(\mathcal{O}) \simeq I_K(\mathfrak{f})/P_{K,\mathbb{Z}}(\mathfrak{f}).$$

LEMMA 2.4. *We have the isomorphism*

$$\begin{aligned} \langle T_{K,N}, tI_2 \mid t \in (\mathbb{Z}/N\mathbb{Z})^\times \rangle / T_{K,N} &\xrightarrow{\sim} \text{Gal}(K_{\mathfrak{f}}/H_{\mathcal{O}}) \\ tI_2 &\mapsto (h(\tau_K) \mapsto h^{tI_2}(\tau_K) \mid h(\tau) \in \mathcal{F}_N \text{ is finite at } \tau_K). \end{aligned}$$

PROOF. See [6, Proposition 5.3] or [3, Proposition 3.8]. \square

REMARK 2.5. Thus we obtain that

$$\begin{aligned} \text{Gal}(H_{\mathcal{O}}/H_K) &\simeq \text{Gal}(K_{\mathfrak{f}}/H_K)/\text{Gal}(K_{\mathfrak{f}}/H_{\mathcal{O}}) \\ &\simeq (W_{K,N}/T_{K,N})/(\langle T_{K,N}, tI_2 \mid t \in (\mathbb{Z}/N\mathbb{Z})^\times \rangle / T_{K,N}) \\ &\simeq W_{K,N}/\langle T_{K,N}, tI_2 \mid t \in (\mathbb{Z}/N\mathbb{Z})^\times \rangle. \end{aligned}$$

LEMMA 2.6. *Let $h(\tau)$ be a meromorphic modular function on $\Gamma_0(N)$ with rational Fourier coefficients. If $h(\tau)$ is finite at τ_K , then $h(\tau_K)$ lies in $H_{\mathcal{O}}$.*

PROOF. Since $h(\tau_K)$ belongs to $K_{\mathfrak{f}}$ by (5), it suffices to show by Lemma 2.4 that every tI_2 with $t \in (\mathbb{Z}/N\mathbb{Z})^\times$ leaves $h(\tau_K)$ fixed. Decompose tI_2 into $tI_2 = \begin{bmatrix} 1 & 0 \\ 0 & t^2 \end{bmatrix} \begin{bmatrix} t & 0 \\ 0 & t^{-1} \end{bmatrix}$ in $\text{GL}_2(\mathbb{Z}/N\mathbb{Z})$, and let $\tilde{\alpha} \in \text{SL}_2(\mathbb{Z})$ be a preimage of $\begin{bmatrix} t & 0 \\ 0 & t^{-1} \end{bmatrix} \in \text{SL}_2(\mathbb{Z}/N\mathbb{Z})$ with respect to the reduction $\text{SL}_2(\mathbb{Z}) \rightarrow \text{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I_2\}$. Then we know $\tilde{\alpha} \in \Gamma_0(N)$ and achieve that

$$\begin{aligned} h(\tau_K)^{tI_2} &= h^{tI_2}(\tau_K) \quad \text{by Lemma 2.4} \\ &= h^{\begin{bmatrix} 1 & 0 \\ 0 & t^2 \end{bmatrix} \tilde{\alpha}}(\tau_K) \\ &= h^{\tilde{\alpha}}(\tau_K) \quad \text{since } h(\tau) \text{ has rational Fourier coefficients} \\ &= h(\tau_K) \quad \text{because } \tilde{\alpha} \in \Gamma_0(N). \end{aligned}$$

This proves the lemma. \square

PROPOSITION 2.7. *Let $N \geq 2$ be an integer and $g(\tau)$ be the η -quotient described in Proposition 2.3. Then the special value $g(\tau_K)$ belongs to $H_{\mathcal{O}}$ as a real algebraic number.*

PROOF. By Proposition 2.3 and Lemma 2.6, $g(\tau_K)$ lies in $H_{\mathcal{O}}$. Furthermore, since $g(\tau)$ has rational Fourier coefficients with respect to q and $e^{2\pi i \tau_K}$ is a real number, $g(\tau_K)$ is a real algebraic number. \square

3 Characters on class groups

Let N be a positive integer, $\mathfrak{f} = N\mathcal{O}_K$ and

$$\pi_{\mathfrak{f}} : \mathcal{O}_K \rightarrow \mathcal{O}_K/\mathfrak{f}$$

be the canonical homomorphism. Define group homomorphisms

$$\begin{aligned} \tilde{\Phi}_{\mathfrak{f}} : \pi_{\mathfrak{f}}(\mathcal{O}_K)^{\times} &\rightarrow \text{Cl}(\mathfrak{f}) \\ x + \mathfrak{f} &\mapsto [x\mathcal{O}_K], \text{ the class containing } x\mathcal{O}_K \end{aligned}$$

and

$$\tilde{\Psi}_{\mathfrak{f}} : \pi_{\mathfrak{f}}(\mathcal{O}_K)^{\times} \rightarrow I_K(\mathfrak{f})/P_{K,\mathbb{Z}}(\mathfrak{f})$$

as the composition of $\tilde{\Phi}_{\mathfrak{f}}$ and the natural surjection $\text{Cl}(\mathfrak{f}) = I_K(\mathfrak{f})/P_{K,1}(\mathfrak{f}) \rightarrow I_K(\mathfrak{f})/P_{K,\mathbb{Z}}(\mathfrak{f})$.

LEMMA 3.1. *We have*

$$\text{Ker}(\tilde{\Psi}_{\mathfrak{f}}) = \pi_{\mathfrak{f}}(\mathcal{O}_K^{\times})\pi_{\mathfrak{f}}(\mathbb{Z})^{\times}.$$

PROOF. We deduce that

$$\begin{aligned} x + \mathfrak{f} \in \pi_{\mathfrak{f}}(\mathcal{O}_K)^{\times} &\text{ belongs to } \text{Ker}(\tilde{\Psi}_{\mathfrak{f}}) \\ \iff x\mathcal{O}_K &\in P_{K,\mathbb{Z}}(\mathfrak{f}) \\ \iff x\zeta \equiv n &\pmod{\mathfrak{f}} \text{ for some } \zeta \in \mathcal{O}_K^{\times} \text{ and } n \in \mathbb{Z} \text{ prime to } N \\ \iff x + \mathfrak{f} = \zeta^{-1}n + \mathfrak{f} \\ \iff x + \mathfrak{f} &\in \pi_{\mathfrak{f}}(\mathcal{O}_K^{\times})\pi_{\mathfrak{f}}(\mathbb{Z})^{\times}. \end{aligned}$$

This proves the lemma. □

LEMMA 3.2. *Let G be a finite abelian group and H be a subgroup of G . Let $g \in G$ and n be the smallest positive integer such that $g^n \in H$. If χ is a character of H , then it can be extended to a character χ' of G for which $\chi'(g)$ is any n -th root of $\chi(g^n)$.*

PROOF. See [15, Chapter VI]. □

Let \mathfrak{a} be any nontrivial ideal of \mathcal{O}_K and χ be a character of $(\mathcal{O}_K/\mathfrak{a})^{\times}$. Recall that the conductor \mathfrak{f}_{χ} of χ is defined by

$$(7) \quad \mathfrak{f}_{\chi} = \gcd\{\text{nontrivial ideals } \mathfrak{m} \text{ of } \mathcal{O}_K \mid \chi(\alpha + \mathfrak{a}) = 1 \text{ for all } \alpha \in \mathcal{O}_K \text{ such that } \alpha\mathcal{O}_K \text{ is prime to } \mathfrak{a} \text{ and } \alpha \equiv 1 \pmod{\mathfrak{m}}\}.$$

In particular, \mathfrak{f}_{χ} divides \mathfrak{a} .

LEMMA 3.3. *Let $\mathfrak{g} = p^r \mathcal{O}_K$ for a prime p and a positive integer r . Let χ be a non-principal character of $\pi_{\mathfrak{g}}(\mathcal{O}_K)^\times$ which is trivial on $\pi_{\mathfrak{g}}(\mathbb{Z})^\times$. Then the conductor \mathfrak{f}_χ of χ is divisible by every prime ideal factor of $p\mathcal{O}_K$.*

PROOF. Since χ is nonprincipal, the assertion is obvious if p ramifies or is inert in K .

Now let p split in K , so $p\mathcal{O}_K$ has prime ideal factorization $p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$ with $\mathfrak{p} \neq \bar{\mathfrak{p}}$. Without loss of generality we may assume that \mathfrak{p} divides \mathfrak{f}_χ . Suppose on the contrary that $\bar{\mathfrak{p}}$ does not divide \mathfrak{f}_χ , and hence \mathfrak{f}_χ is a nonzero power of \mathfrak{p} . Let α be any element of \mathcal{O}_K such that $\alpha\mathcal{O}_K$ is prime to \mathfrak{g} and $\alpha \equiv 1 \pmod{\bar{\mathfrak{p}}^r}$. Since $\bar{\alpha} \equiv 1 \pmod{\mathfrak{p}^r}$ and \mathfrak{f}_χ divides \mathfrak{p}^r , we get by the definition (7)

$$(8) \quad \chi(\bar{\alpha} + \mathfrak{g}) = 1.$$

On the other hand, since $N_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}$ and χ is trivial on $\pi_{\mathfrak{g}}(\mathbb{Z})^\times$, we find

$$\chi(\alpha + \mathfrak{g})\chi(\bar{\alpha} + \mathfrak{g}) = \chi((\alpha + \mathfrak{g})(\bar{\alpha} + \mathfrak{g})) = \chi(N_{K/\mathbb{Q}}(\alpha) + \mathfrak{g}) = 1.$$

It then follows from (8) that

$$\chi(\alpha + \mathfrak{g}) = 1,$$

which implies that \mathfrak{f}_χ divides $\bar{\mathfrak{p}}^r$. But this contradicts the fact that \mathfrak{f}_χ is a nonzero power of \mathfrak{p} , and so \mathfrak{f}_χ is divisible by both \mathfrak{p} and $\bar{\mathfrak{p}}$. \square

For any intermediate field F of the extension $K_{\mathfrak{f}}/K$ we mean by $\text{Cl}(K_{\mathfrak{f}}/F)$ the subgroup of $\text{Cl}(\mathfrak{f})$ ($\simeq \text{Gal}(K_{\mathfrak{f}}/K)$) corresponding to $\text{Gal}(K_{\mathfrak{f}}/F)$.

LEMMA 3.4. *For an integer $N \geq 2$ with prime factorization $N = \prod_{k=1}^m p_k^{r_k}$, let \mathcal{O} be the order of conductor N in K . Let $C \in \text{Cl}(\mathfrak{f}) \setminus \text{Cl}(K_{\mathfrak{f}}/H_{\mathcal{O}})$ (if any). Assume that the order of the group*

$$G_k = \pi_{p_k^{r_k}\mathcal{O}_K}(\mathcal{O}_K)^\times / \pi_{p_k^{r_k}\mathcal{O}_K}(\mathcal{O}_K^\times) \pi_{p_k^{r_k}\mathcal{O}_K}(\mathbb{Z})^\times$$

is greater than 2 for each $k \in \{1, \dots, m\}$. Then there exists a character χ of $\text{Cl}(\mathfrak{f})$ satisfying

- (i) χ is trivial on $\text{Cl}(K_{\mathfrak{f}}/H_{\mathcal{O}})$,
- (ii) $\chi(C) \neq 1$,
- (iii) every prime ideal factor of \mathfrak{f} divides the conductor \mathfrak{f}_χ of χ .

PROOF. By Lemma 3.2 we can take a character χ of $\text{Cl}(\mathfrak{f})$ satisfying (i) and (ii). Observe that the conductor \mathfrak{f}_χ of χ is defined to be that of the character $\tilde{\chi} = \chi \circ \tilde{\Phi}_{\mathfrak{f}}$ of $\pi_{\mathfrak{f}}(\mathcal{O}_K)^\times$. By the Chinese remainder theorem we have the natural isomorphism

$$\pi_{\mathfrak{f}}(\mathcal{O}_K)^\times \simeq \prod_{k=1}^m \pi_{p_k^{r_k} \mathcal{O}_K}(\mathcal{O}_K)^\times.$$

For each $k \in \{1, \dots, m\}$, let

$$\tilde{\iota}_k : \pi_{p_k^{r_k} \mathcal{O}_K}(\mathcal{O}_K)^\times \hookrightarrow \prod_{k=1}^m \pi_{p_k^{r_k} \mathcal{O}_K}(\mathcal{O}_K)^\times \xrightarrow{\sim} \pi_{\mathfrak{f}}(\mathcal{O}_K)^\times$$

be the natural injection and $\tilde{\chi}_k = \tilde{\chi} \circ \tilde{\iota}_k$. Then it is obvious by the definition (7) that \mathfrak{f}_χ is divisible by $\prod_{k=1}^m \mathfrak{f}_{\tilde{\chi}_k}$. Let \mathcal{O}_k be the order of conductor $p_k^{r_k}$ in K (hence, $H_{\mathcal{O}_k} \subseteq H_{\mathcal{O}}$). By Lemma 3.1 and (6) we obtain an injection

$$\begin{aligned} G_k &\rightarrow I_K(p_k^{r_k} \mathcal{O}_K) / P_{K, \mathbb{Z}}(p_k^{r_k} \mathcal{O}_K) \xrightarrow{\sim} \text{Gal}(H_{\mathcal{O}_k} / K) \xrightarrow{\sim} \text{Gal}(K_{\mathfrak{f}} / K) / \text{Gal}(K_{\mathfrak{f}} / H_{\mathcal{O}_k}) \\ &\xrightarrow{\sim} \text{Cl}(\mathfrak{f}) / \text{Cl}(K_{\mathfrak{f}} / H_{\mathcal{O}_k}). \end{aligned}$$

Thus we may identify G_k with a subgroup of $\text{Cl}(\mathfrak{f}) / \text{Cl}(K_{\mathfrak{f}} / H_{\mathcal{O}_k})$.

Suppose that $\tilde{\chi}_k = 1$ for some $k \in \{1, \dots, m\}$. If we let e_k be the exponent of G_k , then we are faced with two possible cases.

Case 1. First, consider the case $e_k = 2$. Let $[C]$ be the class of C in $\text{Cl}(\mathfrak{f}) / \text{Cl}(K_{\mathfrak{f}} / H_{\mathcal{O}_k})$ and n be the smallest positive integer so that $[C]^n$ belongs to G_k . Since $e_k = 2$ and $|G_k| > 2$ by hypothesis, G_k is not a cyclic group. In particular, $G_k \supsetneq \langle [C]^n \rangle$. Hence there exists a nonprincipal character ψ of G_k such that $\psi([C]^n) = 1$ by Lemma 3.2. And, we can extend ψ to a character ψ' of $\text{Cl}(\mathfrak{f}) / \text{Cl}(K_{\mathfrak{f}} / H_{\mathcal{O}_k})$ in such a way that $\psi'([C]) = 1$ again by Lemma 3.2. Let

$$\psi'' = \psi' \circ (\text{Cl}(\mathfrak{f}) \rightarrow \text{Cl}(\mathfrak{f}) / \text{Cl}(K_{\mathfrak{f}} / H_{\mathcal{O}_k})),$$

which is trivial on $\text{Cl}(K_{\mathfrak{f}} / H_{\mathcal{O}_k})$ and $\psi''(C) = 1$. We then see that $\chi\psi''$ is trivial on $\text{Cl}(K_{\mathfrak{f}} / H_{\mathcal{O}_k})$ (so, on $\text{Cl}(K_{\mathfrak{f}} / H_{\mathcal{O}})$) and

$$(\chi\psi'')(C) = \chi(C)\psi''(C) = \chi(C) \neq 1.$$

Moreover, since $\tilde{\chi}_k = 1$, we get

$$(\chi\psi'') \circ \tilde{\Phi}_{\mathfrak{f}} \circ \tilde{\iota}_k = \psi \circ (\pi_{p_k^{r_k} \mathcal{O}_K}(\mathcal{O}_K)^\times \rightarrow G_k),$$

which is trivial on $\pi_{p_k^{r_k} \mathcal{O}_K}(\mathcal{O}_K^\times) \pi_{p_k^{r_k} \mathcal{O}_K}(\mathbb{Z})^\times$ as a nonprincipal character of $\pi_{p_k^{r_k} \mathcal{O}_K}(\mathcal{O}_K)^\times$. Therefore every prime ideal factor of $p_k \mathcal{O}_K$ divides the conductor $\mathfrak{f}_{\chi\psi''}$ of $\chi\psi''$ by Lemma 3.3. And, we further note that

$$(\chi\psi'') \circ \tilde{\Phi}_{\mathfrak{f}} \circ \tilde{\iota}_\ell = \tilde{\chi}_\ell \quad \text{for all } \ell \in \{1, \dots, m\} \text{ such that } \ell \neq k$$

by the construction of ψ'' . Now, we replace χ by $\chi\psi''$.

Case 2. Next, let $e_k > 2$. Then there is a character ξ of G_k such that $\xi^2 \neq 1$, because the exponent of the character group of G_k is also greater than 2. Extend ξ to a character ξ' of $\text{Cl}(\mathfrak{f})/\text{Cl}(K_{\mathfrak{f}}/H_{\mathcal{O}_k})$ by using Lemma 3.2, and let

$$\xi'' = \xi' \circ (\text{Cl}(\mathfrak{f}) \rightarrow \text{Cl}(\mathfrak{f})/\text{Cl}(K_{\mathfrak{f}}/H_{\mathcal{O}_k})).$$

Then we see that ξ'' is trivial on $\text{Cl}(K_{\mathfrak{f}}/H_{\mathcal{O}_k})$ and $\xi''^2 \neq 1$. Set

$$\rho = \begin{cases} \xi'' & \text{if } \xi''(C) \neq \chi(C)^{-1}, \\ \xi''^2 & \text{if } \xi''(C) = \chi(C)^{-1} (\neq 1). \end{cases}$$

As in the above, one can readily check that $\chi\rho$ is trivial on $\text{Cl}(K_{\mathfrak{f}}/H_{\mathcal{O}})$, $(\chi\rho)(C) \neq 1$, every prime factor of $p_k\mathcal{O}_K$ divides the conductor $\mathfrak{f}_{\chi\rho}$ of $\chi\rho$ and

$$(\chi\rho) \circ \widetilde{\Phi}_{\mathfrak{f}} \circ \widetilde{\iota}_{\ell} = \widetilde{\chi}_{\ell} \quad \text{for all } \ell \in \{1, \dots, m\} \text{ such that } \ell \neq k.$$

Hence, we replace χ by $\chi\rho$.

Continuing this way we eventually obtain a character χ of $\text{Cl}(\mathfrak{f})$ satisfying the conditions (i)~(iii) in the lemma. \square

4 Ring class invariants

For a vector $\begin{bmatrix} r_1 \\ r_2 \end{bmatrix} \in \mathbb{Q}^2 \setminus \mathbb{Z}^2$ we define the *Siegel function* $g_{\begin{bmatrix} r_1 \\ r_2 \end{bmatrix}}(\tau)$ on \mathbb{H} by the following infinite product

$$g_{\begin{bmatrix} r_1 \\ r_2 \end{bmatrix}}(\tau) = -q^{(1/2)(r_1^2 - r_1 + 1/6)} e^{\pi i r_2(r_1 - 1)} (1 - q^{r_1} e^{2\pi i r_2}) \prod_{n=1}^{\infty} (1 - q^{n+r_1} e^{2\pi i r_2}) (1 - q^{n-r_1} e^{-2\pi i r_2}).$$

If $M (\geq 2)$ is an integer so that $Mr_1, Mr_2 \in \mathbb{Z}$, then $g_{\begin{bmatrix} r_1 \\ r_2 \end{bmatrix}}(\tau)^{12M}$ belongs to \mathcal{F}_M and has neither zeros nor poles on \mathbb{H} [8, Chapter 2, Theorem 1.2].

Let \mathfrak{f} be a nontrivial proper ideal of \mathcal{O}_K and $C \in \text{Cl}(\mathfrak{f})$. Let $N = N(\mathfrak{f}) (\geq 2)$ be the smallest positive integer in \mathfrak{f} . Take any integral ideal $\mathfrak{c} \in C$ and let

$$\begin{aligned} \mathfrak{f}\mathfrak{c}^{-1} &= [\omega_1, \omega_2] \quad \text{for some } \omega_1, \omega_2 \in \mathbb{C} \text{ such that } \omega_1/\omega_2 \in \mathbb{H}, \\ 1 &= (a/N)\omega_1 + (b/N)\omega_2 \quad \text{for some } a, b \in \mathbb{Z}. \end{aligned}$$

We define the *Siegel-Ramachandra invariant* $g_{\mathfrak{f}}(C)$ of conductor \mathfrak{f} at the class C by

$$g_{\mathfrak{f}}(C) = g_{\begin{bmatrix} a/N \\ b/N \end{bmatrix}}(\omega_1/\omega_2)^{12N},$$

which depends only on \mathfrak{f} and C , not on the choice of \mathfrak{c} , ω_1 and ω_2 [8, Chapter 11, §1]. It lies in $K_{\mathfrak{f}}$ and satisfies the transformation formula

$$(9) \quad g_{\mathfrak{f}}(C)^{\sigma_{\mathfrak{f}}(C')} = g_{\mathfrak{f}}(CC') \quad \text{for any } C' \in \text{Cl}(\mathfrak{f}),$$

where $\sigma_{\mathfrak{f}} : \text{Cl}(\mathfrak{f}) \rightarrow \text{Gal}(K_{\mathfrak{f}}/K)$ is the Artin reciprocity map [8, Chapter 11, Theorem 1.1]. Ramachandra [11] further showed that $g_{\mathfrak{f}}(C)$ is an algebraic integer and a unit if \mathfrak{f} is not a power of one prime ideal (see also [7, §3]).

For a nonprincipal character χ of $\text{Cl}(\mathfrak{f})$ we define the *Stickelberger element* and the *L-function* as

$$S_{\mathfrak{f}}(\chi) = \sum_{C \in \text{Cl}(\mathfrak{f})} \chi(C) \ln |g_{\mathfrak{f}}(C)| \quad \text{and} \quad L_{\mathfrak{f}}(s, \chi) = \sum_{\substack{\mathfrak{a} : \text{nontrivial ideals of } \mathcal{O}_K \\ \text{prime to } \mathfrak{f}}} \frac{\chi([\mathfrak{a}])}{N_{K/\mathbb{Q}}(\mathfrak{a})^s} \quad (s \in \mathbb{C}),$$

respectively.

PROPOSITION 4.1 (The second Kronecker limit formula). *Let \mathfrak{f}_{χ} be the conductor of χ and χ_0 be the proper character of $\text{Cl}(\mathfrak{f}_{\chi})$ corresponding to χ . If $\mathfrak{f}_{\chi} \neq \mathcal{O}_K$, then we have*

$$L_{\mathfrak{f}_{\chi}}(1, \chi_0) \prod_{\mathfrak{p} | \mathfrak{f}, \mathfrak{p} \nmid \mathfrak{f}_{\chi}} (1 - \overline{\chi}_0([\mathfrak{p}])) = - \frac{\pi \chi_0([\gamma \mathfrak{d}_K \mathfrak{f}_{\chi}])}{3N(\mathfrak{f}_{\chi}) \sqrt{-d_K} \omega(\mathfrak{f}_{\chi}) T_{\gamma}(\overline{\chi}_0)} S_{\mathfrak{f}}(\overline{\chi}),$$

where \mathfrak{d}_K is the different of K/\mathbb{Q} , γ is an element of K so that $\gamma \mathfrak{d}_K \mathfrak{f}_{\chi}$ becomes an integral ideal of K prime to \mathfrak{f}_{χ} , $\omega(\mathfrak{f}_{\chi}) = |\{\zeta \in \mathcal{O}_K^{\times} \mid \zeta \equiv 1 \pmod{\mathfrak{f}_{\chi}}\}|$ and

$$T_{\gamma}(\overline{\chi}_0) = \sum_{x + \mathfrak{f}_{\chi} \in \pi_{\mathfrak{f}_{\chi}}(\mathcal{O}_K)^{\times}} \overline{\chi}_0([x \mathcal{O}_K]) e^{2\pi i \text{Tr}_{K/\mathbb{Q}}(x\gamma)}.$$

PROOF. See [9, Chapter 22, Theorems 1 and 2] and [8, Chapter 11, Theorem 2.1]. \square

REMARK 4.2. (i) If every prime ideal factor of \mathfrak{f} divides \mathfrak{f}_{χ} , then we understand the Euler factor $\prod_{\mathfrak{p} | \mathfrak{f}, \mathfrak{p} \nmid \mathfrak{f}_{\chi}} (1 - \overline{\chi}_0([\mathfrak{p}]))$ to be 1.

(ii) Since χ_0 is a nonprincipal character of $\text{Cl}(\mathfrak{f}_{\chi})$, we get $L_{\mathfrak{f}_{\chi}}(1, \chi_0) \neq 0$ [4, Chapter V, Theorem 10.2].

(iii) The Gauss sum $T_{\gamma}(\overline{\chi}_0)$ is nonzero, in particular, $|T_{\gamma}(\overline{\chi}_0)| = \sqrt{N_{K/\mathbb{Q}}(\mathfrak{f}_{\chi})}$ [9, Chapter 22, §1].

Now, let $\mathfrak{f} = N\mathcal{O}_K$ for some integer N (≥ 2) with prime factorization $N = \prod_{k=1}^m p_k^{r_k}$. Let \mathcal{O} be the order of conductor N in K . Here we follow the notations stated in (3) and (4).

LEMMA 4.3. *Let C_0 be the identity class of $\text{Cl}(\mathfrak{f})$. Then we have*

$$N_{K_{\mathfrak{f}}/H_{\mathcal{O}}}(g_{\mathfrak{f}}(C_0))^{\min\{2, N-1\}} = \nu_N^{12N} \prod_{S \subseteq \{1, \dots, m\}} \Delta((N/P_S)\tau_K)^{(-1)^{|S|}N},$$

which is an algebraic integer.

PROOF. See [3, Theorem 4.2]. □

THEOREM 4.4. *Assume that the order of the group*

$$\pi_{p_k^{r_k} \mathcal{O}_K}(\mathcal{O}_K)^{\times} / \pi_{p_k^{r_k} \mathcal{O}_K}(\mathcal{O}_K^{\times}) \pi_{p_k^{r_k} \mathcal{O}_K}(\mathbb{Z})^{\times}$$

is greater than 2 for each $k \in \{1, \dots, m\}$. Then the special value

$$(10) \quad \nu_N^{12\mu_N / \gcd(24, P_N)} \prod_{S \subseteq \{1, \dots, m\}} \eta((N/P_S)\tau_K)^{24(-1)^{|S|}\mu_N / \gcd(24, P_N)}$$

generates $H_{\mathcal{O}}$ over K as a real algebraic integer.

PROOF. Let C_0 be the identity class of $\text{Cl}(\mathfrak{f})$ and $\varepsilon = N_{K_{\mathfrak{f}}/H_{\mathcal{O}}}(g_{\mathfrak{f}}(C_0))^{\ell}$ for a nonzero integer ℓ . Suppose that $F = K(\varepsilon)$ is properly contained in $H_{\mathcal{O}}$, so we can take a class $C \in \text{Cl}(K_{\mathfrak{f}}/F) \setminus \text{Cl}(K_{\mathfrak{f}}/H_{\mathcal{O}})$. By Lemma 3.4 we know that there exists a character χ of $\text{Cl}(\mathfrak{f})$ for which χ is trivial on $\text{Cl}(K_{\mathfrak{f}}/H_{\mathcal{O}})$, $\chi(C) \neq 1$ and every prime ideal factor of \mathfrak{f} divides the conductor \mathfrak{f}_{χ} of χ . Then we see from Proposition 4.1 and Remark 4.2 that the Stickelberger element $S_{\mathfrak{f}}(\tilde{\chi})$ is nonzero.

On the other hand, we derive that

$$\begin{aligned} S_{\mathfrak{f}}(\bar{\chi}) &= \sum_{\substack{C_1 \in \text{Cl}(\mathfrak{f}) \\ C_1 \bmod \text{Cl}(K_{\mathfrak{f}}/F)}} \sum_{\substack{C_2 \in \text{Cl}(K_{\mathfrak{f}}/F) \\ C_2 \bmod \text{Cl}(K_{\mathfrak{f}}/H_{\mathcal{O}})}} \sum_{C_3 \in \text{Cl}(K_{\mathfrak{f}}/H_{\mathcal{O}})} \bar{\chi}(C_1 C_2 C_3) \ln |g_{\mathfrak{f}}(C_1 C_2 C_3)| \\ &= \sum_{C_1} \bar{\chi}(C_1) \sum_{C_2} \bar{\chi}(C_2) \sum_{C_3} \bar{\chi}(C_3) \ln |g_{\mathfrak{f}}(C_0)^{\sigma_{\mathfrak{f}}(C_1) \sigma_{\mathfrak{f}}(C_2) \sigma_{\mathfrak{f}}(C_3)}| \quad \text{by (9)} \\ &= \sum_{C_1} \bar{\chi}(C_1) \sum_{C_2} \bar{\chi}(C_2) \sum_{C_3} \ln |g_{\mathfrak{f}}(C_0)^{\sigma_{\mathfrak{f}}(C_1) \sigma_{\mathfrak{f}}(C_2) \sigma_{\mathfrak{f}}(C_3)}| \quad \text{since } \chi \text{ is trivial on } \text{Cl}(K_{\mathfrak{f}}/H_{\mathcal{O}}) \\ &= \sum_{C_1} \bar{\chi}(C_1) \sum_{C_2} \bar{\chi}(C_2) \ln |N_{K_{\mathfrak{f}}/H_{\mathcal{O}}}(g_{\mathfrak{f}}(C_0))^{\sigma_{\mathfrak{f}}(C_1) \sigma_{\mathfrak{f}}(C_2)}| \\ &= (1/\ell) \sum_{C_1} \bar{\chi}(C_1) \ln |\varepsilon^{\sigma_{\mathfrak{f}}(C_1)}| \sum_{C_2} \bar{\chi}(C_2) \quad \text{by the fact } \varepsilon = N_{K_{\mathfrak{f}}/H_{\mathcal{O}}}(g_{\mathfrak{f}}(C_0))^{\ell} \in F \\ &= 0, \end{aligned}$$

because χ can be viewed as a nonprincipal character of $\text{Cl}(K_{\mathfrak{f}}/F)/\text{Cl}(K_{\mathfrak{f}}/H_{\mathcal{O}})$. This yields a contradiction, and hence we achieve $H_{\mathcal{O}} = F = K(N_{K_{\mathfrak{f}}/H_{\mathcal{O}}}(g_{\mathfrak{f}}(C_0))^{\ell})$.

Finally, the special value in (10) becomes a generator of $H_{\mathcal{O}}$ over K as a real algebraic integer by Lemmas 2.6 and 4.3. This completes the proof. □

REMARK 4.5. Let $\mathfrak{g} = p^r \mathcal{O}_K$ for a prime p and a positive integer r , and consider the group

$$G = \pi_{\mathfrak{g}}(\mathcal{O}_K)^{\times} / \pi_{\mathfrak{g}}(\mathcal{O}_K^{\times}) \pi_{\mathfrak{g}}(\mathbb{Z})^{\times}.$$

We have the order formulas

$$\begin{aligned} |\pi_{\mathfrak{g}}(\mathcal{O}_K)^{\times}| &= p^{2(r-1)}(p-1) \left(p - \left(\frac{d_K}{p} \right) \right), \\ |\pi_{\mathfrak{g}}(\mathcal{O}_K^{\times}) \pi_{\mathfrak{g}}(\mathbb{Z})^{\times}| &= (|\mathcal{O}_K^{\times}|/2) p^{r-1} (p-1), \end{aligned}$$

where $\left(\frac{d_K}{p} \right)$ stands for the Kronecker symbol.

$$\left(\frac{d_K}{p} \right) = \begin{cases} \text{the Legendre symbol} & \text{if } p \text{ is odd,} \\ \text{the Kronecker symbol} & \text{if } p = 2 \end{cases}$$

[1, p.148]. Then we achieve

$$|G| = \frac{2p^{r-1}}{|\mathcal{O}_K^{\times}|} \left(p - \left(\frac{d_K}{p} \right) \right).$$

And, one can classify all the cases in which $|G| = 1$ or 2 as listed in Table 1:

K	$\mathbb{Q}(\sqrt{-1})$	$\mathbb{Q}(\sqrt{-3})$	neither $\mathbb{Q}(\sqrt{-1})$ nor $\mathbb{Q}(\sqrt{-3})$			
			$d_K \equiv 1 \pmod{24}$	$d_K \equiv 9, 17 \pmod{24}$	$d_K \equiv 13 \pmod{24}$	otherwise
p^r	$2, 2^2, 3, 5$	$2, 2^2, 3, 5, 7$	$2, 2^2, 3$	$2, 2^2$	$2, 3$	2

Table 1: The cases $|G| = 1$ or 2

5 Examples

In this last section, we shall present some examples of computing minimal polynomials of ring class invariants with relatively small coefficients developed in Theorem 4.4 so as to apply them to quadratic Diophantine equations concerning non-convenient numbers.

EXAMPLE 5.1. Let $K = \mathbb{Q}(\sqrt{-1})$, so $d_K = -4$ and $\tau_K = \sqrt{-1}$. In this case, we have $H_K = K$. Let \mathcal{O} be the order of conductor 13 in K . Then the special value $13(\eta(13\tau_K)/\eta(\tau_K))^2$ generates $H_{\mathcal{O}}$ over K as a real algebraic integer by Theorem 4.4 and Remark 4.5. And, we attain by Remark 2.5 that

$$\begin{aligned} \text{Gal}(H_{\mathcal{O}}/K) &\simeq W_{K,13} / \langle T_{K,13}, tI_2 \mid t \in (\mathbb{Z}/13\mathbb{Z})^{\times} \rangle \\ &= \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} \begin{bmatrix} 1 & -1 \\ -6 & 7 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 5 \end{bmatrix} \begin{bmatrix} 1 & -2 \\ 3 & -5 \end{bmatrix}, \right. \\ &\quad \left. \begin{bmatrix} 1 & 0 \\ 0 & 10 \end{bmatrix} \begin{bmatrix} 1 & -3 \\ -1 & 4 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 11 \end{bmatrix} \begin{bmatrix} 14 & -33 \\ 3 & -7 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 4 \end{bmatrix} \begin{bmatrix} 1 & 4 \\ -1 & -3 \end{bmatrix} \right\}, \end{aligned}$$

from which we can compute (by using Maple ver.15)

$$\begin{aligned}
& \min(13(\eta(13\tau_K)/\eta(\tau_K))^2, K) \\
&= (X - 13(\eta(13\tau)/\eta(\tau))^2 \circ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}(\tau_K))(X - 13(\eta(13\tau)/\eta(\tau))^2 \circ \begin{bmatrix} 1 & -1 \\ -6 & 7 \end{bmatrix}(\tau_K)) \\
&\quad (X - 13(\eta(13\tau)/\eta(\tau))^2 \circ \begin{bmatrix} 1 & -2 \\ 3 & -5 \end{bmatrix}(\tau_K))(X - 13(\eta(13\tau)/\eta(\tau))^2 \circ \begin{bmatrix} 1 & -3 \\ -1 & 4 \end{bmatrix}(\tau_K)) \\
&\quad (X - 13(\eta(13\tau)/\eta(\tau))^2 \circ \begin{bmatrix} 14 & -33 \\ 3 & -7 \end{bmatrix}(\tau_K))(X - 13(\eta(13\tau)/\eta(\tau))^2 \circ \begin{bmatrix} 1 & 4 \\ -1 & -3 \end{bmatrix}(\tau_K)) \\
&= X^6 + 10X^5 + 46X^4 + 108X^3 + 122X^2 + 38X - 1.
\end{aligned}$$

On the other hand, by using the relation

$$j(\tau) = (2^8\eta(2\tau)^{16}\eta(\tau)^{-16} + \eta(2\tau)^{-8}\eta(\tau)^8)^3$$

[1, pp.256–257], one can also get

$$\begin{aligned}
\min(j(13\tau_K), K) &= X^6 - 10368X^5 + 44789760X^4 - 103195607040X^3 \\
&\quad + 133741506723840X^2 - 92442129447518208X \\
&\quad + 26623333280885243904.
\end{aligned}$$

Here we observe that the coefficients of $\min(13(\eta(13\tau_K)/\eta(\tau_K))^2, K)$ are relatively smaller than those of $\min(j(13\tau_K), K)$.

EXAMPLE 5.2. Let $K = \mathbb{Q}(\sqrt{-7})$, so $d_K = -7$ and $\tau_K = (-1 + \sqrt{-7})/2$. Then we know $H_K = K$, too.

- (i) Let \mathcal{O} be the order of conductor 7 in K . Then the special value $7^2(\eta(7\tau_K)/\eta(\tau_K))^4$ generates $H_{\mathcal{O}}$ over K as a real algebraic integer by Theorem 4.4 and Remark 4.5. And, we derive by Remark 2.5

$$\begin{aligned}
\text{Gal}(H_{\mathcal{O}}/K) &\simeq W_{K,7}/\langle T_{K,7}, tI_2 \mid t \in (\mathbb{Z}/7\mathbb{Z})^\times \rangle \\
&= \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} \begin{bmatrix} -1 & -2 \\ 4 & 7 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} \begin{bmatrix} 7 & -2 \\ 11 & -3 \end{bmatrix}, \right. \\
&\quad \left. \begin{bmatrix} 1 & 0 \\ 0 & 4 \end{bmatrix} \begin{bmatrix} 1 & 5 \\ 2 & 11 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 2 & 5 \\ 1 & 3 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} -3 & 5 \\ 1 & -2 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 4 \end{bmatrix} \begin{bmatrix} 5 & 12 \\ 2 & 5 \end{bmatrix} \right\}
\end{aligned}$$

and obtain

$$\begin{aligned}
& \min(7^2(\eta(7\tau_K)/\eta(\tau_K))^4, K) \\
&= (X - 7^2(\eta(7\tau)/\eta(\tau))^4 \circ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}(\tau_K))(X - 7^2(\eta(7\tau)/\eta(\tau))^4 \circ \begin{bmatrix} -1 & -2 \\ 4 & 7 \end{bmatrix}(\tau_K)) \\
&\quad (X - 7^2(\eta(7\tau)/\eta(\tau))^4 \circ \begin{bmatrix} 7 & -2 \\ 11 & -3 \end{bmatrix}(\tau_K))(X - 7^2(\eta(7\tau)/\eta(\tau))^4 \circ \begin{bmatrix} 1 & 5 \\ 2 & 11 \end{bmatrix}(\tau_K)) \\
&\quad (X - 7^2(\eta(7\tau)/\eta(\tau))^4 \circ \begin{bmatrix} 2 & 5 \\ 1 & 3 \end{bmatrix}(\tau_K))(X - 7^2(\eta(7\tau)/\eta(\tau))^4 \circ \begin{bmatrix} -3 & 5 \\ 1 & -2 \end{bmatrix}(\tau_K)) \\
&\quad (X - 7^2(\eta(7\tau)/\eta(\tau))^4 \circ \begin{bmatrix} 5 & 12 \\ 2 & 5 \end{bmatrix}(\tau_K)) \\
&= X^7 + 21X^6 + 175X^5 + 679X^4 + 1162X^3 + 490X^2 + 588X + 7.
\end{aligned}$$

(ii) Now, let \mathcal{O} be the order of conductor 6. We know by Remark 2.5 that

$$\begin{aligned}\mathrm{Gal}(H_{\mathcal{O}}/K) &\simeq W_{K,6}/\langle T_{K,6}, tI_2 \mid t \in (\mathbb{Z}/6\mathbb{Z})^\times \rangle \\ &= \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 5 & 2 \\ 2 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 3 & -2 \\ 2 & -1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ -2 & -3 \end{bmatrix} \right\},\end{aligned}$$

which is of order 4. Set $h(\tau) = (\eta(6\tau)\eta(\tau)/\eta(3\tau)\eta(2\tau))^{12}$. Since $h(\tau_K) \in \mathbb{R}$, we deduce that

$$\begin{aligned}[K(h(\tau_K)) : K] &= [K(h(\tau_K)) : \mathbb{Q}]/[K : \mathbb{Q}] \\ &= [K(h(\tau_K)) : \mathbb{Q}(h(\tau_K))][\mathbb{Q}(h(\tau_K)) : \mathbb{Q}]/[K : \mathbb{Q}] \\ &= [\mathbb{Q}(h(\tau_K)) : \mathbb{Q}].\end{aligned}$$

Furthermore, we see that the polynomial

$$\begin{aligned}&\prod_{\gamma \in \mathrm{Gal}(H_{\mathcal{O}}/K)} (X - h(\tau_K)^\gamma) \\ &= (X - h(\tau) \circ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}(\tau_K))(X - h(\tau) \circ \begin{bmatrix} 5 & 2 \\ 2 & 1 \end{bmatrix}(\tau_K)) \\ &\quad (X - h(\tau) \circ \begin{bmatrix} 3 & -2 \\ 2 & -1 \end{bmatrix}(\tau_K))(X - h(\tau) \circ \begin{bmatrix} 1 & 2 \\ -2 & -3 \end{bmatrix}(\tau_K)) \\ &= X^4 - 35X^3 + 198X^2 + 4060X + 1\end{aligned}$$

is irreducible over \mathbb{Q} . Hence $h(\tau_K) = (\eta(6\tau_K)\eta(\tau_K)/\eta(3\tau_K)\eta(2\tau_K))^{12}$ generates $H_{\mathcal{O}}$ over K as a unit, although we couldn't directly apply Theorem 4.4 to this case. This example indicates that there seems to be a room for the condition on the order of the group $\pi_{p_k^{r_k}\mathcal{O}_K}(\mathcal{O}_K)^\times / \pi_{p_k^{r_k}\mathcal{O}_K}(\mathcal{O}_K^\times) \pi_{p_k^{r_k}\mathcal{O}_K}(\mathbb{Z})^\times$ to be improved further.

EXAMPLE 5.3. Let $K = \mathbb{Q}(\sqrt{-6})$. We then have $d_K = -24$ and $\tau_K = \sqrt{-6}$. Let \mathcal{O} be the order of conductor 3 in K . Then the real algebraic integer $3^6(\eta(3\tau_K)/\eta(\tau_K))^{12}$ generates $H_{\mathcal{O}}$ over K by Theorem 4.4 and Remark 4.5. And, we see by Remark 2.5 that

$$\mathrm{Gal}(H_{\mathcal{O}}/H_K) \simeq W_{K,3}/\langle T_{K,3}, tI_2 \mid t \in (\mathbb{Z}/3\mathbb{Z})^\times \rangle = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right\}.$$

However, in this case, $H_K \neq K$. On the other hand, as is well-known $\mathrm{Gal}(H_K/K)$ is isomorphic to the form class group $C(d_K)$ of discriminant $d_K = -24$ which consists of two reduced primitive positive definite quadratic forms

$$Q_1 = X^2 + 6Y^2 \quad \text{and} \quad Q_2 = 2X^2 + 3Y^2$$

[1, Theorems 2.8, 5.23 and 7.7]. Corresponding to Q_1 and Q_2 we let

$$\beta_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \tau_1 = \sqrt{-6} \quad \text{and} \quad \beta_2 = \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}, \tau_2 = \sqrt{-6}/2,$$

respectively. Then due to Steinhagen [17] the Galois conjugates of $h(\tau_K)$, where $h(\tau) = 3^6(\eta(3\tau)/\eta(\tau))^{12}$, are given by

$$h^{\gamma\beta_k}(\tau_k) \quad \text{for } \gamma \in \text{Gal}(H_O/H_K) \text{ and } k = 1, 2$$

(see also [5, Theorem 2.4]). And, we achieve

$$\begin{aligned} & \{\gamma\beta_k \mid \gamma \in \text{Gal}(H_O/H_K), k = 1, 2\} \quad (\subseteq \text{GL}_2(\mathbb{Z}/3\mathbb{Z})/\{\pm I_2\}) \\ &= \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} \begin{bmatrix} -1 & 0 \\ 1 & -1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} \begin{bmatrix} -1 & 0 \\ 2 & -1 \end{bmatrix} \right\}, \end{aligned}$$

from which we get

$$\begin{aligned} & \min(3^6(\eta(3\tau_K)/\eta(\tau_K))^{12}, K) \\ &= (X - h(\tau) \circ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}(\sqrt{-6}))(X - h(\tau) \circ \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}(\sqrt{-6}))(X - h(\tau) \circ \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}(\sqrt{-6})) \\ & \quad (X - h(\tau) \circ \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}(\sqrt{-6}/2))(X - h(\tau) \circ \begin{bmatrix} -1 & 0 \\ 1 & -1 \end{bmatrix}(\sqrt{-6}/2)) \\ & \quad (X - h(\tau) \circ \begin{bmatrix} -1 & 0 \\ 2 & -1 \end{bmatrix}(\sqrt{-6}/2)) \\ &= X^6 + 234X^5 + 39015X^4 + 1335852X^3 + 14036895X^2 - 4833270X + 729. \end{aligned}$$

REMARK 5.4. Let n be a positive integer and $f_n(X) \in \mathbb{Z}[X]$ be the minimal polynomial of a real algebraic integer which generates the ring class field of the order $\mathbb{Z}[\sqrt{-n}]$ in the imaginary quadratic field $\mathbb{Q}(\sqrt{-n})$. Then we have the assertion that if an odd prime p divides neither n nor the discriminant of $f_n(X)$, then p can be written in the form $p = x^2 + ny^2$ for some $x, y \in \mathbb{Z}$ if and only if $(\frac{-n}{p}) = 1$ and $f_n(X) \equiv 0 \pmod{p}$ has an integer solution as well [1, Theorem 9.2]. Whenever the equivalent condition cannot be expressed as $p \equiv c_1, \dots, c_m \pmod{4n}$, we call such n a non-convenient number. As for the convenient numbers we refer to [1, §3.C], [18] and [19].

- (i) We are able to use our ring class invariants in Examples 5.1 and 5.3 for these quadratic Diophantine problems. First, let $K = \mathbb{Q}(\sqrt{-1})$ (, so $\tau_K = \sqrt{-1}$). Then we get

$$\text{disc}(13(\eta(13\tau_K)/\eta(\tau_K))^2, K) = 2^{10} \cdot 3^6 \cdot 13^5,$$

and derive that a prime p satisfies $(\frac{-169}{p}) = 1$ if and only if $p = 2$ or $p \equiv 1 \pmod{4}$. Thus we reach the conclusion that if p is a prime other than 13, then p can be written in the form $p = x^2 + 169y^2$ for some $x, y \in \mathbb{Z}$ if and only if $p \equiv 1 \pmod{4}$ and $X^6 + 10X^5 + 46X^4 + 108X^3 + 122X^2 + 38X - 1 \equiv 0 \pmod{p}$ has an integer solution.

Second, let $K = \mathbb{Q}(\sqrt{-6})$ (, so $\tau_K = \sqrt{-6}$). We compute

$$\text{disc}(3^6(\eta(3\tau_K)/\eta(\tau_K))^{12}, K) = 2^{69} \cdot 3^{36} \cdot 13^4 \cdot 17^2 \cdot 19^4 \cdot 23^2,$$

and find that a prime p satisfies $(\frac{-54}{p}) = 1$ if and only if $p \equiv 1, 5, 7, 11 \pmod{24}$. Thus we can conclude that a prime p can be written in the form $p = x^2 + 54y^2$ for some $x, y \in \mathbb{Z}$ if and only if $p \equiv 1, 5, 7, 11 \pmod{24}$ and $X^6 + 234X^5 + 39015X^4 + 1335852X^3 + 14036895X^2 - 4833270X + 729 \equiv 0 \pmod{p}$ has an integer solution.

- (ii) In like manner, one can further show by using Example 5.2(ii) that a prime p can be expressed as $p = x^2 + 63y^2$ for some $x, y \in \mathbb{Z}$ if and only if $p \equiv 1, 9, 11 \pmod{14}$ and $X^4 - 35X^3 + 198X^2 + 4060X + 1 \equiv 0 \pmod{p}$ has an integer solution.

References

- [1] D. A. Cox, *Primes of the form $x^2 + ny^2$: Fermat, Class Field, and Complex Multiplication*, John Wiley & Sons, Inc., New York, 1989.
- [2] A. Enge and R. Schertz, *Constructing elliptic curves over finite fields using double eta-quotients*, J. Theor. Nombres Bordeaux 16 (2004), no. 3, 555–568.
- [3] I. S. Eum, J. K. Koo and D. H. Shin, *Ring class invariants over imaginary quadratic fields*, <http://arxiv.org/abs/1007.2309>.
- [4] G. J. Janusz, *Algebraic Number Fields*, 2nd edition, Grad. Studies in Math. 7, Amer. Math. Soc., Providence, R. I., 1996.
- [5] H. Y. Jung, J. K. Koo and D. H. Shin, *Ray class invariants over imaginary quadratic fields*, Tohoku Math. J. (2) 63 (2011), no. 3, 413–426.
- [6] J. K. Koo and D. H. Shin, *Function fields of certain arithmetic curves and application*, Acta Arith. 141 (2010), no. 4, 321–334.
- [7] J. K. Koo and D. H. Shin, *On some arithmetic properties of Siegel functions*, Math. Zeit. 264 (2010), no. 1, 137–177.
- [8] D. Kubert and S. Lang, *Modular Units*, Grundlehren der mathematischen Wissenschaften 244, Springer-Verlag, 1981.
- [9] S. Lang, *Elliptic Functions*, With an appendix by J. Tate, 2nd edition, Grad. Texts in Math. 112, Springer-Verlag, New York, 1987.
- [10] K. Ono, *The Web of Modularity: Arithmetic of the Coefficients of Modular Forms and q -series*, CBMS Regional Conf. Series in Math. 102, Amer. Math. Soc., Providence, R. I., 2004.

- [11] K. Ramachandra, *Some applications of Kronecker's limit formula*, Ann. of Math. (2) 80 (1964), 104–148.
- [12] R. Schertz, *Zur Theorie der Ringklassenkörper über imaginär-quadratischen Zahlkörpern*, J. Number Theory 10 (1978), no. 1, 70–82.
- [13] R. Schertz, *Construction of ray class fields by elliptic units*, J. Théor. Nombres Bordeaux 9 (1997), no. 2, 383–394.
- [14] R. Schertz, *Complex multiplication*, New Math. Monographs 15, Cambridge University Press, Cambridge, 2010.
- [15] J.-P. Serre, *A Course in Arithmetic*, Grad. texts in Math., Springer-Verlag, New York-Heidelberg, 1973.
- [16] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Iwanami Shoten and Princeton University Press, Princeton, N. J., 1971.
- [17] P. Stevenhagen, *Hilbert's 12th problem, complex multiplication and Shimura reciprocity*, Class Field Theory-Its Centenary and Prospect (Tokyo, 1998), 161–176, Adv. Stud. Pure Math. 30, Math. Soc. Japan, Tokyo, 2001.
- [18] A. Weil, *Number Theory: An Approach Through History; From Hammurapi to Legendre*, Birkhäuser Boston, Inc., Boston, MA, 1984.
- [19] P. J. Weinberger, *Exponents of the class groups of complex quadratic fields*, Acta Arith. 22 (1973), 117–124.

DEPARTMENT OF MATHEMATICAL SCIENCES
KAIST
DAEJEON 305-701
REPUBLIC OF KOREA

E-mail address: jkkoo@math.kaist.ac.kr

DEPARTMENT OF MATHEMATICS
HANKUK UNIVERSITY OF FOREIGN STUDIES
YONGIN-SI, GYEONGGI-DO 449-791
REPUBLIC OF KOREA

E-mail address: dhshin@hufs.ac.kr

NATIONAL INSTITUTE FOR MATHEMATICAL
SCIENCES
DAEJEON 305-811
REPUBLIC OF KOREA

E-mail address: dsyoon@nims.re.kr